National Institutes of Health

Office of the Senior Official for Privacy

Privacy

Frequently Asked Questions (FAQs)

Table of Contents

Privacy Act

1. What is Privacy?

Privacy can be summed up in one word: *Trust*

It's the ability to control who has access to information and to whom that information is communicated.

Adoption of privacy principles ensures federal agencies balance individual, organizational, and societal interests. Failure to protect personal information can have serious, real-life consequences.

Privacy Fair Information Practice Principles (FIPPs):

Access and Amendment: NIH should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

Accountability: NIH should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to all employees and contractors who have access to PII.

Authority: NIH should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

Minimization: NIH should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

Quality and Integrity: NIH should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Individual Participation: NIH should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. NIH should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

Purpose Specification and Use: NIH should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Security: NIH should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Transparency: NIH should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2. Why is Privacy Important?

Privacy is an essential freedom. It is the right of individuals to determine for themselves when, how, and to what extent personal information in the possession of NIH and its contractors is communicated to others.

Security is the protection of NIH data from accidental or intentional, and unauthorized modification, destruction, or disclosure.

The loss of personally identifiable information (PII), Privacy Act information, sensitive information (SI), Controlled Unclassified Information (CUI), and protected health information (PHI) can have a serious, severe or catastrophic adverse effect on:

- Individuals to whom the information pertains
- Organizational operations and assets

A breach of privacy can occur when you lose information you are entrusted to protect, destroy information willingly or misuse your position to disclose information improperly to someone unauthorized to receive it.

3. What are the different Types of Private Information?

NIH employees, direct and third-party contractors, and affiliates working on behalf of the Federal Government handle many different types of personal information on a daily basis. Know the difference between the five main types of information we must protect. NIH is responsible for protecting different types of information:

Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information

Personally Identifiable Information (PII) is defined by OMB A-130[1] as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Some types of PII present more risks to individuals if the information is compromised. To mitigate these risks, some types of PII require additional safeguarding mechanisms that would be too burdensome for non-sensitive PII. These stricter handling guidelines are laid out in the HHS Sensitive PII Memo[2] for limiting the increased risk to an individual if the data is compromised.

[1] Office of Management and Budget; OMB A-130, Managing Federal Information as a Strategic Resource

[2] HHS Sensitive PII Definition and Guidance Memorandum

Examples of PII:

- Name
- Photographic identifier
- Fingerprint/voiceprint
- Vehicle identifier
- Personal mailing/phone/email address
- Medical record number
- Medical notes
- Certificates, legal documents
- Device identifiers, web URL
- IP address (when collected with regard to a particular transaction)
- Military status
- Foreign activities
- Identifier that identifies, locates or contacts an individual
- Identifier that reveals activities, characteristics or details about a person

Examples of Data Elements that are always Sensitive PII:

- Social Security Number
- Driver's License Number
- Medical Records Number
- Alien Registration Number
- Taxpayer Identification Number
- Biometric Identifiers

Examples of Data Elements that are Sensitive PII when in combination with other PII:

- Date of Birth
- Last four of a SSN
- Mother's Maiden Name
- Sexual Orientation
- Citizenship or Immigration Status
- Passport Number

Protected Health Information (PHI)

Protected Health Information, or PHI is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

Examples:

- Name
- Geographical Sub-Divisions smaller than a State, including Street Address, City, County, Precinct, Zip Code (and their equivalent Geo-Codes)
- Account Numbers
- Certificate/License Numbers
- Device Identifiers/Serial Numbers
- Web URLs
- IP Address Numbers

- Elements of Dates (except year)
- Phone & Fax Numbers
- Email Addresses
- SSNs (full number and last 4 digits)
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Biometric Identifiers (including finger and voice prints)
- Full Face Photographic and Comparable Images
- Other unique identifying number, characteristic, or code (except the unique code assigned by a Principal Investigator to code data)

Sensitive Information

Information is considered **"sensitive"** if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Controlled Unclassified Information

Is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended[3].

4. When can Social Security Numbers be Collected?

- SSNs must only be collected or used if such collections are (1) required or authorized by law or (2) required by HHS and/or NIH operational necessities[4].In accordance with the HHS IS2P[5], system owners must consult with the Office of General Counsel (OGC) and the NIH Senior Official for Privacy (SOP) to determine whether the proposed collection of PII is legally authorized and that there is a link between the authorization and the specific collection of PII. Proper documentation of the legal authority to collect SSN can be done via a PIA, system of records notice (SORN), or an SSN Justification Memorandum. Solicitation of an SSN is protected by law
- OMB Memo M-17-12[6] requires agencies to reduce and/or eliminate the unnecessary use of SSNs
- The full SSN is a unique identifier, as are the last 4 digits
- Use of an alternate identifier is recommended
- Executive Order 9397 as amended by E.O. 13478, states that the SSN "may" be used as the enumerator, when a program-specific statute or E.O. permits or requires use of an enumerator or other method to distinguish between individuals.

Q: "My office uses a form that requests an individual's Social Security Number, but the SSN isn't really necessary for our office to conduct its business. What should I do?"

[3] NIST 800-171 Rev.2

[4] HHS Social Security Number (SSN) Reduction and Elimination Memorandum

[5] HHS Information Systems Security and Privacy Policy

[6] Office of Management and Budget; M 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

A: Remove it! Work with the appropriate supervisors and/or forms manager to have the SSN removed from the form.

Q: Are the last 4 digits of a SSN considered to be PII?

A: Yes, although a truncated SSN can reduce the risk to the individual if compromised, it can still be used to identify the individual.

5. Where do Privacy laws Originate?

The Privacy Act[7], as amended, was enacted in 1974. The Electronic Government (E-Gov) Act[8] was enacted in 2002 as was the Federal Information Security Management Act (Title III of the E-Gov Act)[9].

In addition to these statutes, NIH must also comply with various Office of Management and Budget (OMB) Memoranda and HHS and NIH Information Security and Privacy Policies.

In part, the Privacy Act requires agencies to:

- Limit the collection of personal information to what is necessary
- Publish a Systems of Record Notice (SORN) prior to storing information in a record system designed to be retrieved by a personal identifier

- Prior to operating a record system subject to the Privacy Act, a SORN must be approved by the Office of Management and Budget and the Department and Congress for 30 days. Then published in the Federal Register for an additional 30 days to allow for public comment.
- Contact your IC Privacy Coordinator to determine whether a SORN needs to be created.
- Visit the NIH Office of Management Assessment Privacy Website for a list of current NIH SORNs[10]

- Comply with the law or face civil remedies and criminal penalties

    - Civil remedies can be applied if NIH fails to comply with the Privacy Act in such a way as to have an adverse effect on an individual. Violations can include:
    - Refusing to amend an individual's record in accordance with his request;
    - Possession of or access to agency records which contain PII, the disclosure of which is prohibited;
    - Knowingly disclosing agency material in any manner;
    - Failing to maintain a record that is accurate, timely, and complete to assure fairness of any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made that is adverse to the individual;
    - Failing to comply with a provision or rule that results in an adverse effect on the individual.

[7] Privacy Act of 1974

[8] E Government Act of 2002

[9] Federal Information Security Modernization Act of 2014

[10] NIH Office of Management Assessment Privacy Website

- Criminal penalties (misdemeanor charge, jail time, fines, and court costs) can be applied if you as an officer or employee of NIH, or by virtue of your employment or official position, commit a violation under the Privacy Act. Violations can include:
- Possession of or access to agency records which contain PII, the disclosure of which is prohibited;
- Knowingly disclosing agency material in any manner to any person or agency not entitled to receive it;
- Willfully maintaining an illegal system of records prior to publication of a System Notice in the Federal Register;
- Sharing data with unauthorized individuals; and,
- Obtaining or disclosing data under false pretenses or facilitating others acting under false pretenses.

The E-Gov Act requires agencies to:

- Conduct **Privacy Impact Assessments** for NIH **entities**

  - A Privacy Impact Assessment (PIA) is a risk mitigation tool that provides a documented process to identify and protect both employee and public data. The PIA is completed using a standard template, in coordination with the IC Privacy Coordinator and ISSO, by the person within the IC who manages the system, holds the account or understands the characteristics of the entity. Other key stakeholders may be involved. The PIA is approved internally and submitted to the Office of the Senior Official for Privacy for review/approval prior to submission to the Department.
  - NIH requires a PIA for the following entities:
  - IT Systems that are FISMA Reportable – General Support Systems and Major Stand-Alone applications that are owned or operated by NIH or on behalf of the agency, whether hosted at NIH or off-site by a commercial vendor, contractor or cloud provider. Examples: CRIS, IMPAC II, ITAS, NED.
  - IT Systems, components, and Surveys that store PII – Electronic information collections or online survey tools that contain personal information about members of the public or non-work related information about NIH employees. Examples: EDie, SurveyMonkey/Gizmo, Project Implicit.
  - Uses of Third-Party Websites and Applications – Web-based technologies not exclusively operated or controlled by a government entity, or which involve the significant participation of a non-government entity. Often, these technologies are located on a .COM website or other location that is not part of an official government domain. They can also be embedded or incorporated on an NIH website. Examples: Facebook, LinkedIn, Pinterest, Twitter, YouTube, and Instagram

- Translate **privacy policies** into standardized machine-readable format

  - The Privacy Policy is a single, centrally located statement that is accessible from an IC's official homepage, application or paper form used to collect information from members of the public. It should be a consolidated explanation of the IC's general privacy-related practices.
  - It should specify how the IC will use PII made available to NIH, who will have access to it, with whom it will be shared outside of NIH, whether and how long NIH intends to maintain the PII, how NIH will secure the PII it uses or maintains, what other privacy risks may exist and how NIH will mitigate them.

- Post **privacy notices** on public-facing agency websites

  - The Privacy Notice is a brief description of how the IC's Privacy Policy will apply in a specific situation. It should serve to notify individuals before they engage with NIH and should be provided on the specific webpage, application or paper form where individuals have the opportunity to make PII available to NIH.
  - The phrase "make PII available" includes any NIH action that causes PII to become available or accessible to NIH, whether or not NIH solicits or collects it. In general, an individual can make PII available to us when s/he provides, submits, communicates, links, posts or associates PII while using our websites, applications or paper forms. "Associate" can include activities commonly referred to as "friending," "following," "liking," "joining a group," becoming a "fan," and comparable functions.

FISMA requires agencies to:

- Provide a comprehensive framework for IT standards and programs
- Ensure integrity, confidentiality and availability of personal information
- Perform program management, evaluation, and OMB reporting activities

6. Why have a Privacy Act?

- We have a constitutional right to privacy. Amendment IV of the U.S. Constitution says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…";
- Information is affected by the collection, maintenance, use and dissemination by Federal agencies; and
- The use of the internet, computers, and other technology create the possibility for faster and greater distribution, which could lead to greater harm.

7. What does the Privacy Act do?

- Limits the collection of personal information;
- Prevents secret Government record systems;
- Prevents secret use of Government records;
- States individual's right to see and correct records;
- Requires safeguards to be implemented to protect the security and accuracy of the information; and
- Allows for civil remedies and criminal penalties to be assessed for violations under the Privacy Act.

8. Who does the Privacy Act cover and not cover?

- The Privacy Act covers:
    - U.S. citizens
    - Resident aliens
- The Privacy Act does not cover:
    - Non-resident aliens
    - The deceased
    - Organizations

9. When is NIH allowed to collect my information?

- NIH may not legally maintain records on individuals unless:
    - The information is relevant and necessary to accomplish an NIH or Department function required by statute or Executive Order;
    - The information in the record is acquired to the greatest extent practicable directly from the subject individual; and
    - The individual providing the record is informed when the record is collected under the authority NIH has for requesting the record.

10. When are a supervisor's notes considered agency records?

- Supervisor notes are agency records when they are:
    - Used as the basis for an employment action; and
    - Otherwise made a part of an employee's personnel file and treated as official agency documentation.
- Supervisor notes are NOT agency records when they are:
    - The personal property of the supervisor only;
    - Never circulated or shared with others;
    - Never passed to replacement supervisors or those acting in the absence of the supervisor;
    - Used as memory joggers only; and
    - Not used as official agency documentation.

11. What is a Privacy Act Records System?

- A group of records (more than one), not available in the public domain;
- A record that contains information about an individual that is personal in nature (i.e., name, age, sex, gender, ethnicity, home address, phone, SSN, medical credentials, medical, financial and/or educational background, etc.); and
- A record designed to be retrieved by the individual's name, or another personal identifier such as an ID number, protocol number, photo, fingerprint, etc.

12. What is a System of Records Notice (SORN)?

- A document posted in the Federal Register that notifies the public of the existence and what information is contained in a specific system,
- How that information is collected, used, maintained, and disseminated in relation to other systems; and
- A SORN also explains how individuals may gain access to information about themselves.
- Listing of NIH SORNs is available on the HHS Privacy Program website.

13. How do I submit a records request?

- An individual who wishes to request a specific record must submit a request **in writing** to the appropriate NIH Institute or Center (IC) that collected and maintains that record;
- The written request should be as specific as possible. Please describe what type of information was collected, who collected it, why it was collected, when it was collected, and, if known, who (individual or organization) collected it; and

14. How do I amend an incorrect record?

- An individual who notices that a record is incorrect must submit a request **in writing** to the appropriate NIH IC that collected and maintains that record;
- The written notice should include the current record and provide an accurate correction of the record; and

15. Can I appeal the denial to access or correct my information?

- Requesters who wish to appeal NIH's decision to deny access to correct or amend his or her record must do so within 30 days of the receipt of a decision letter from NIH. Appeals should include the following information:
    - Reasons why the requested information should be corrected or amended under the Act; and
    - Why the denial may be in error.

- Requesters wishing to submit an appeal to a denial of access should attach to their appeal, a copy of their original request and response letter, clearly mark the letter and the outside envelope "Privacy Act Appeal" and mail the documents to the following address:

  Deputy Agency Chief FOIA Officer

  U.S. Department of Health and Human Services

  Office of the Assistant Secretary for Public Affairs

  Room 729H

  200 Independence Avenue, S.W.

- Washington, DC 20201Reuestors wishing to discuss their issues before filing an appeal to attempt to resolve a dispute without going through the appeals process, individuals may contact the HHS FOIA Public Liaison for assistance at:

  HHS FOIA/PA Public Liaison

  FOI/Privacy Acts Division

  Assistant Secretary for Public Affairs (ASPA)

  Office of the Secretary (OS)

  U.S. Department of Health and Human Services (HHS)

  200 Independence Avenue, SW, Suite 729H

  Washington, DC 20201

- Requesters wishing to submit an appeal to a denial of amendment should create a response letter to the denial of amendment and email the document to the IC Privacy Coordinator or OSOP Privacy Analyst that they have been working with. The NIH Privacy Act Officer will work with the requestor, IC Privacy Coordinator, and the Immediate Office of the Director to draft a Memorandum to be sent to the NIH Principal Director for review and decision.

16. Are there circumstances in which certain information cannot be released?

- NIH will provide access to records within their possession unless one of the exceptions or exemptions applies:

  - The records contain information about a third party;
  - Information that is not about the subject of the file, and therefore not accessible under the Privacy Act;
  - Records were compiled in reasonable anticipation of a civil action or proceeding;
  - Records are maintained by the CIA; or
  - Records are maintained by an agency or component thereof, which performs as its principal function any activity pertaining to the enforcement of criminal laws.

17. Where can I find information regarding the Paperwork Reduction Act (PRA) / Office of Management and Budget (OMB) Clearance procedures?

- NIH PRA/OMB Website[11]:
- The Paperwork Reduction Act (PRA) of 1995 requires agencies to obtain approval from OMB prior to soliciting and/or obtaining identical information from ten or more members of the public in multiple forms. PRA/OMB approval is required whether the Federal agency collects the information itself or uses an outside agent or contractor. OMB requires 90-120 days to approve new information collections and renew existing approvals.
- You can go to the NIH Office of Extramural Research (OER) Intranet website[12] to obtain a list of NIH PRA/OMB Project Clearance Liaisons,and get more information about whether your IT system has been approved for PRA/OMB information collection.

18. Where can I find information about the HIPAA Privacy Rule?

- For additional information on a wide range of topics about the Health Insurance Portability and Accountability (HIPAA) Privacy Rule, please visit the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Privacy Rule Web Site[13]. You can also call the OCR Privacy toll-free phone line at (866) 627-7748. Information about OCR's civil rights authorities and responsibilities can be found on the OCR home page.

19. Where can I find guidance regarding the HIPAA Privacy Rule and the Electronic Exchange of Health Information?

- Though NIH is not a HIPAA covered entity, individuals can find the HHS OCR has published new HIPAA Privacy Rule guidance as part of the Department's Privacy and Security Toolkit to implement *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Privacy and Security Framework). The Privacy and Security Framework and Toolkit is designed to establish privacy and security principles for health

[11] The Paperwork Reduction Act (PRA) of 1995

[12] NIH Office of Extramural Research (OER)

[13] U.S. Department of Health and Human Services Office for Civil Rights

care stakeholders engaged in the electronic exchange of health information and includes tangible tools to facilitate implementation of these principles. The new HIPAA Privacy Rule guidance in the Toolkit discusses how the Privacy Rule supports and can facilitate electronic health information exchange in a networked environment. In addition, the guidance includes documents that address electronic access by an individual to his or her protected health information and how the Privacy Rule may apply to and supports the use of Personal Health Records. HIPAA guidance documents are available at the HHS Office for Civil Rights' webpage. For more information on the HIPAA Privacy Rule visit the HHS OCR FAQ webpage.

20. Can I subscribe to an electronic listserv in order to receive information sent directly to my email inbox?

- **Yes**. The HHS OCR operates an announce-only electronic list serv as a resource to distribute information about the HIPAA Privacy Rule. It is named OCR-Privacy-list. To subscribe to or unsubscribe from the list serv, please go to HHS OCR's Covered Entities Listserv webpage[14]:

21. Who can I contact if a person or organization covered by the Privacy Rule violates my health information privacy rights?

- NIH does not meet the definition of a "covered entity" and is therefore not covered by HIPAA because it does not bill third parties for the health care they receive at the Clinical Center. However, if you believe that a person or organization outside of NIH who is covered by the Privacy Rule (a "covered entity") violated your health information privacy rights or otherwise violated the Privacy Rule, you may file a complaint with OCR. For additional information about how to file a complaint, see the OCR's Fact Sheet "How to File a Health Information Privacy Complaint".

22. Where can I find information about the Family Educational Rights and Privacy Act (FERPA) regulation and other helpful information?

- FERPA is a Federal law that protects the privacy of students' "education records." (See 20 U.S.C. § 1232g; 34 CFR Part 99). The HIPAA Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information and gives patients a right over their health information. The guidance is available at HHS OCR's HIPAA webpage. Information about the Family Policy Compliance Office (FPCO) is available at the U.S. Department of Education's website[15].

[14] HHS OCR Listserv

[15] Family Educational Rights and Privacy Act (FERPA)

23. Where can I find U.S. Department of Health and Human Services (HHS) and U.S. Department of Education (ED) joint guidance on the application of FERPA and HIPAA to Student Health Records?

- The Departments of Education and Health and Human Services have jointly released guidance to explain the relationship between the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, and to address apparent confusion on the part of school administrators, health care professionals, and others as to how these two laws apply to student health records. The guidance also addresses certain disclosures that are allowed without consent or authorization under both laws, especially those disclosures related to health and safety emergency situations. The guidance was developed in response to the "Report to the President on Issues Raised by the Virginia Tech Tragedy" (June 13, 2007) as well as to address questions the respective Departments have heard generally from stakeholders regarding the intersection of the HIPAA Privacy Rule and FERPA. The Departments of Health and Human Services and Education are committed to a continuing dialogue with school officials and other professionals on these important matters affecting the safety and security of our nation's schools. While this guidance seeks to answer many questions that school officials and others have had about the intersection of these federal laws, ongoing discussions may cause more issues to emerge.

Federal Information Security Management Act (FISMA)/ Privacy Impact Assessments (PIAs)

1. What is FISMA's purpose?

- Inform and raise awareness among Federal agency heads of the importance of information security programs;
- Facilitate the development of security programs through mandatory comprehensive reporting and evaluation; and
- Ensure that federal agencies take the necessary precautions to secure agency IT systems and protect personally identifiable information (PII) and mitigate the risk of a breach to PII.

2. What are the major components of the FISMA Section III report?

- Inventory of Systems that Contain Federal Information in Identifiable Form which require a Privacy Impact Assessment (PIA) or System of Records Notice (SORN);
- Links to PIAs and SORNs;
- Senior Agency Official for Privacy (SAOP) Responsibilities;
- Information Privacy Training and Awareness;
- PIA and Web Privacy Policies and Processes;
- Conduct of Mandated Reviews;
- Policy Compliance (pursuant with OMB Circulars A-130 and A-108[16], along with OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information);

[16] Office of Management and Budget; OMBA-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act

- Agency Use of Persistent Tracking Technology; and
- Privacy Points of Contact.

3. What is the FISMA report process/timeline?

- While FISMA compliance is an ongoing process, which requires quality reviews, the final annual report is due at the end of the Federal fiscal year (September 30);
- All FISMA report data is collected approximately two months in advance of the report deadline in order to compile the data and promote it, through the Department, to the Inspector General; and
- Agencies must continually monitor IT systems and privacy procedures and responsibilities to ensure that OPDIVs are compliant with Federal IT and privacy laws.

4. What is a PIA?

- A means to assure compliance with applicable privacy laws and regulations;
- An evaluation tool used to determine the risks and effects of collecting, maintaining and disseminating personally identifiable information (PII) in an electronic Information Technology (IT) System used by multiple users (e.g., network, server, database) or through the use of a Third-Party Website or Application (TPWA);
- An analysis instrument to enable system developers and system owners/managers to identify and evaluate privacy risks; and
- A tool that evaluates:

    - Data in the IT System or TPWA;
    - Attributes of the Data;
    - Access to the Data;
    - Information Collection and Use Practices;
    - Privacy Notice Practices;
    - Information Sharing and Maintenance Practices;
    - If the IT System Contains Federal Records;
    - Whether the Use Creates or Modifies a Privacy Act System of Records;
    - Whether the Use Creates an Information Collection under the Paperwork Reduction Act;
    - Website Hosting and Uses of TPWAs to Collect or Maintain Data;
    - Maintenance of Administrative & Technical and Physical Controls; and
    - Management and disposition requirements per Records Retention Schedules

- Parts of a PIA include:

    - Date of Submission;
    - Agency/OPDIV/IC;
    - Title of System;
    - Existing, New or Modified;
    - Unique PIA Identifier;
    - System of Records Number;
    - OMB Info Collection Approval Number & Expiration Date;
    - Other Identifiers;
    - System Overview;
    - Legislative Authority;

- How will information be collected;
- How will ICO use the information;
- Why is information collected;
- With whom will the information be shared;
- From whom will the information be collected;
- What will subjects be told about the collection;
- How will the message be conveyed;
- What are opportunities for consent;
- Will information be collected from children under 13 on the internet? If so, how will parental approval be obtained;
- How will information be secured; and
- How will information be retained and destroyed

5. Why do we conduct PIAs?

- To comply with the E-Government Act, OMB guidance, HHS policy and supporting guidance that requires all IT Systems and each use of a TPWA, whether already in existence, development, or undergoing modification;
- To help determine what type of information is collected by IT systems and Third-Party Websites and Applications throughout NIH;
- To decide which precautions need to be implemented to protect such information;
- To provide privacy stakeholders an orderly process in which they can report IT system collected information to the SOP; and
- To have an orderly process for submitting IT system information related to privacy for FISMA reporting.

6. Which IT Systems or TPWAs Need a PIA?

- IT systems owned, operated, maintained, or controlled by the Federal government or a contracted company working on behalf of the agency;
- Web-based technologies that are not exclusively operated or controlled by a government entity, or that involve significant participation of a non-government entity;
- IT systems and TPWAs that maintain government data;
- Those that have not been assessed previously;
- Those in development (as part of the certification and accreditation [C&A] process); and,
- Those assessed previously which have undergone a “major change”.

7. What is a Major Change?

A “major change” is a modification to an IT System or TPWA that affects the following:

- Security and/or Privacy controls
- Type of data collected
- IT System or TPWA interconnection
- Information sharing
- Business processes

Examples of Major Changes

- Conversions: When converting paper-based records to electronic IT Systems or TPWAs.
- Anonymous to Non-Anonymous: When functions applied to an existing information collection change anonymous information into PII.
- Significant IT System or TPWA Management Changes: When new uses, including application of new technologies, significantly change how PII is managed in the IT System or TPWA.
- Significant Merging: When agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- New Public Access: When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic IT System or TPWA.

8. Who Should Prepare/Review/Approve PIAs?

- PIAs are completed by an IT System or TPWA Owner/Manager in consultation with the IC Privacy Coordinator, ISSO, Web Master, Paperwork Reduction Act (PRA) Liaison, Records Liaison and other key stakeholders, as applicable, via NSAT.
- They are distributed through the respective ICO and NIH organizational channels for concurrence (i.e., Supervisory Chain/Executive Officers).
- The NIH Senior Official for Privacy (SOP) will review, approve, and date each PIA and promote it to the Department.
- On a quarterly basis, HHS will post a summary of the IT System or TPWA PIA on a public website[17].
- The HHS OCIO will communicate to the NIH SOP the status of PIAs not approved for posting

9. When do I fill out the entire PIA vs. an Internal PIA vs. a PIA Summary (Privacy Threshold Analysis)?

- If the system for which the PIA is being completed collects PII, the entire PIA form must be completed.
- If the system for which the PIA is being completed collects only PII of federal staff and direct contractors, the entire PIA form must be completed and HHS will deem the PIA an Internal PIA.

If it does NOT collect PII, you only need to complete the PIA Summary (first 14 questions, plus questions starting at 40 if there is a public facing website).NOTE If the IT system is deemed an Internal PIA or PTA, HHS will not post the HHS Approved assessment to their website for public consumption.

10. How do I determine if a system collects PII?

- PII is defined as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual;
- If any of these, or any other categories of information that can be linked to an individual, are stored, maintained, passed through, or disseminated by the system, the system collects PII; and

[17] HHS PIA and TPWA

- IC Privacy Coordinators should be able to validate whether or not a system collects PII based on the information provided to them by System Owners/Managers.

11. Must I complete a new PIA for an existing IT system each year?

- A new PIA is not required if information has been previously assessed under a similar evaluation, or if the system has not undergone any major changes as defined in OMB M-03-22[18]; and
- All existing PIAs must be reviewed for accuracy each year This annual review should be documented by the IC Privacy Coordinator. The annual review will help to meet several Privacy Controls (i.e., DM-1c, DM-2a, and SE-1a from NIST 800-53 Rev.4)

12. Are there any quick tips that would make PIA completion easier?

- Leverage OSOP provided Cheat Sheets, Best Practices, and Umbrella PIAs;
- Consult with other privacy stakeholders as appropriate (e.g. IC Privacy Coordinator, IC Chief Information Officer and ISSOs) when questions about PIAs, privacy, or other questions arise;
- Ensure that your answers are accurate and complete (specifically answer the questions, provide sufficient detail, spell out acronyms, check spelling etc.);
- Remember that PIAs, with public PII, are published to a HHS public facing website;
- Avoid contradicting answers. For example, do not deny that the system collects Social Security Numbers (SSN) and then later claim that the system retrieves information using SSN;
- System Owners/Managers should work with IC Privacy Coordinators and ISSOs early in the System Development Life Cycle to ensure that the PIA process is properly incorporated;
- Know the business objective of the system; and
- Know the difference between privacy and security

[18] Office of Management and Budget; M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

PIA Form

1. What is a PIA Unique Identifier and how can I find one?

The PIA Unique Identifier is an HHS Security Data Warehouse (HSDW)-generated number. This number is assigned when the OSOP analyst creates the HSDW PIA form in HSDW or already exist from a previous submission. ***2. What is a System of Records Notice (SORN) and where can I find one?***

- A SORN describes the Privacy Act system of records, and the categories of PII collected, maintained, retrieved, and used within the system. It provides information to the public on various characteristics of the system (e.g. description, purpose, data collection, notification, retention and disposal, etc.) and how NIH intends to manage and protect the system. The SORN Number is that which is assigned to the Privacy Act SORN (also referred to as the Systems Notice)

  NOTE: If the system is subject to the Privacy Act, then a SORN must be cited as an answer in the PIA.

- All NIH SORNs are located on HHS Privacy Program webpage.

3. What is an OMB Information Collection Approval Number?

- The Paperwork Reduction Act (PRA) of 1995 requires agencies to obtain approval from OMB prior to soliciting and/or obtaining identical information from ten or more members of the public in multiple forms. PRA/OMB approval is required whether the Federal agency collects the information itself or uses an outside agent or contractor. OMB requires 90-120 days to approve new information collections and renew existing approvals. The OMB Information Collection Approval Number should be identical to the one OMB assigned pursuant to having been filed under the Paperwork Reduction Act and is sometimes referred to as an OMB control number. It would only apply if the system maintains data as part of an approved OMB information collection from 10 or more members of the general public; and
- You can click on the Office of Extramural Research (OER) Intranet website[19] to obtain a list of NIH PRA/OMB Project Clearance Liaisons and get more information about whether your IT system has been approved for PRA/OMB information collection.

[19] NIH Office of Extramural Research (OER) Intranet website for PRA Project liaisons

4. Are there policies or guidelines in place with regard to the retention and destruction of PII?

- For Privacy Act systems of records, records retention and disposal procedures should be indicated within the SORN cited for the system. If the system is not subject to the Privacy Act and does not have a SORN in place, consult with the ICO Records Liaison to ascertain the appropriate records retention and disposal schedule for the system. A list of IC Records Liaisons can be accessed from OMA's webpage[20].

Web Privacy

1. Where can I find HHS Machine-Readable Privacy Policy?

- At HHS Digital Communications Division's 508 Compliancy webpage.[21]

2. Who do I contact if a user inquires about the web site's privacy standards?

- Please contact your IC Privacy Coordinator if you have any questions regarding a web site's privacy standards, procedures, or requirements. If you do not know who your IC Privacy Coordinator is, please refer to the NIH Office of Management Assessment's Privacy webpage.[22]

3. Can I post a new web site or update an existing web site before it complies with NIH web privacy requirements?

- No. ICs must comply with NIH web privacy policies before posting a new web site or revising an existing one. See NIH Web Page Privacy Policy – NIH Manual Chapter 2805[23]

4. Does Section 508 compliance apply to emails?

- Section 508 or machine-readability compliance applies to website design and page information, documents available on the website (such as forms, newsletters and brochures), and on-line systems used both for internal and external purposes. Emails sent in text format can generally be read by everyone. If they include web links, the fully qualifying URL should be shown as well, including the 'http://www' part.

  However, Section 508 does apply to email messages, ***particularly*** those which are sent to larger groups, often referred to as 'broadcast mailings.' The current HHS standard with links to more information is available at the HHS Digital Communications Division's Web Standards website[24].

[20] NIH Office of Management and Assessment IC Records Liaison list

[21] HHS Digital Communications Division

[22] NIH Office of Management and Assessment Privacy IC Coordinator list

[23] NIH Office of Management and Assessment Manual Chapter 2805

[24] HHS Web Standards

The Department standard generally states, "HHS must make email accessible to persons with disabilities. All emails—internal or external—as well as their attachments, including graphics, audio, and video must be accessible." In terms of e-mails that are sent to smaller and known audiences, HHS states that these e-mails "**should** meet Section 508 standards as much as practicable. Alternative or accessible formats ["accommodations"] must be made available upon request." Questions about Section 508 Compliance can be directed to the NIH Section 508 Help inbox located at the NIH Office of the Chief Information Officer's IT Governance & Policy webpage[25].

Privacy Incident and Breach Response

1. What is a Privacy Incident?

A privacy incident is the act of violating an explicit or implied privacy policy. It can be caused by misuse and abuse of organizational resources, human error, a physical attack or theft, or a hacking intrusion. It can be unintentional, deliberate and malicious or inappropriate but not malicious. It can involve more than one type of PII. Examples include:

- Disclosure of an individual's place and date of birth to the wrong individual via a website;
- Sending a full or partial SSN unencrypted via e-mail;
- Uploading personnel records electronically via an HR system to the wrong employee;
- Placing employee emergency contact information on a shared network drive;
- Losing an unencrypted portable storage device containing financial account information;
- Witnessing an unauthorized individual remove criminal records from an office;
- Mailing medical records to the wrong doctor or patient;
- Faxing access and authentication information to someone via an unsecure fax machine;
- Disposing of sensitive records in a trash can rather than a shred or burn box; and,
- Surplusing/leasing/removing copiers, printers, scanners and fax machines before a memory wipe/disk sanitization is complete

2. What is a Security Incident?

A ***security incident*** is An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.. Examples include:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data;
- Unwanted disruption or denial of service;
- Unauthorized use of a system for the processing or storage of data; and
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

[25] NIH Office of the Chief Information Officer's IT Governance & Policy webpage

3. What is a Breach?

A breach is any successful compromise of any level of protective controls to, or unauthorized access to or use of, systems or data. An attempt, successful or unsuccessful, is an incident, making a breach a subset of incidents.

The terms *"breach"* and *"privacy incident"* are sometimes used interchangeably. Often, the breaches that make it into the news and receive special attention are those that involve PII. This is because privacy breaches or security breaches that involve PII require extra steps (such as notification to individuals).

A ***breach (as it relates to PII)*** is the loss control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses **personally identifiable information** for an other than authorized purpose. ~ Defined in OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information.*

A ***breach (as it relates to PHI)*** is the unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information ~ Defined in the *American Recovery and Reinvestment Act of 2009.*

All suspected or confirmed incidents and breaches should be reported to the NIH IT Service Desk (301-496-4357) or your ICO Information Systems Security Officer (ISSO) within one hour of discovery.

4. What are some examples of paper and electronic breaches?

- Paper Breach:
  - Having hardcopy documents containing PII stolen from one's desk;
  - Losing a briefcase that contained hardcopy documents containing PII; and
  - Intentionally sharing hardcopy documents that contain PII without authorization.
- Electronic Breach:
  - Unauthorized users gain access to electronic documents containing PII via sharing of passwords, leaving work station unlocked/unattended, etc.;
  - PII is posted, in any format, onto the world wide web without authorization; and
  - Having a laptop containing PII lost or stolen.
  - A laptop or portable storage device storing PII is lost or stolen.

5. Is truncated, redacted, or masked information still considered PII?

- Truncated, redacted, or masked information should still be considered PII. Truncation, redaction, or masking information is a way to protect PII and reduce risk in the event that the PII is lost or compromised.

6. Is encrypted information still considered PII?

- Encrypted information should still be considered PII. Encryption is a way to protect PII and reduce risk in the event that the PII is lost or compromised.

All PII, SI,PHI, and CUI sent via email within NIH and outside the agency must be encrypted.

The five NIH approved methods for sending encrypted e-mail are:

Method and Recommended Use	Permitted Data	Recipient Types	PIV Card Required	Maximum Size	Permissions Required	Shared Mailboxes *	Message Retention	More Information
Office 365 Message Encryption (OME) *Preferred encryption method for all non-medical messages under 150 MB, regardless of recipient*	PHI, PII, SI	Internal or external *Approved for clinician to clinician messages, not clinician to patient*	No	150 MB	No permissions required for Office 365 users	Can send and receive	Permanent	OME FAQs
Secure Email/File Transfer (SEFT)*Preferred encryption method for all non-medical messages over 150 MB, regardless of recipient*	PHI, PII, SI	Internal or external *Approved for clinician to clinician messages, not clinician to patient*	No	200 GB account storage limit	Sender and receiver must register and log in to SEFT	Can't send or receive	30 days	General Information on SEFT
Secure/Multipurpose Internet Mail Extensions (S/MIME) and PIV-D *Legacy encryption methods that use a PIV card to encrypt via laptop and phone respectively -OME is preferred*	PHI, PII, SI	Internal only *Approved for clinician to clinician messages, not clinician to patient*	Yes	100-120MB	Sender and receiver both need valid PKI certificates	Can't send or receive	Permanent	S/MIME Encryption MobileIron: Derived PIV (PIV-D) FAQs
Secure Health Messaging (SHM)*Preferred method for messages between NIH care providers and from care providers to patients (messages attach to CRIS medical records by default)*	PHI, PII, SI	Internal or external *Approved for clinician to patient messages*	No	No file transfer permitted – messaging only	For intramural use only – sender and receiver must log in to the EHR/patient portal	Can't sender receive	Permanent	Clinical Center SHM Training
Medical Secure Email (MSE)*Preferred method for messages from NIH care providers to patients (allows attachment of files, messages are not automatically attached to medical records in CRIS)*	PHI, PII, SI	Internal or external *Approved for clinician to patient messages*	No	200 GB account storage limit	For intramural use only - sender and receiver must log in to MSE	Can't sender receive	3 years	Secure Mail User Guide

7. Is information about employees or direct and third-party contractors considered PII?

- Yes. Information that can be used to distinguish or trace the identity of an employee or contractor should be considered PII.

8. What about information that can be found easily through the Internet or a telephone book (e.g., name, address, or telephone number) …is that PII?

- While a lot of information about a person can be found on the Internet or through other public sources, such as a telephone book, any information provided to the Agency about the public or employees is considered PII. There is an expectation, supported by specific regulatory obligations, that this information will be used as authorized and that it will be protected from loss or compromise. Note that these regulatory obligations even apply to those pieces of information that can easily be found through public sources.

9. I just sent an e-mail containing PII to the wrong person…is that a privacy breach?

- Sending PII to a wrong person via e-mail, whether inside NIH or outside of NIH, is a common situation that an employee can encounter. This situation constitutes a privacy breach. If this situation happens to you, you must report the issue within one hour of discovery to:
  - The IT Service Desk;
  - Your ICO ISSO; and
  - Your Supervisor

10. I just lost a USB thumb-drive with PII on it. Luckily, it was encrypted…is that a privacy breach?

- Losing equipment, such as an encrypted USB thumb-drive, is a situation that should be immediately reported. The NIH IRT, PIRT and IC Privacy Coordinators with the ICO ISSO will work together to assess the incident, determine how to respond, and key next steps. Your role is to report the situation.

11. I work with someone who always provides more information than is requested…sometimes even including a SSN when it is not needed…what should I do?

- You are correct to be concerned. All employees have a responsibility to protect PII and this includes the concept of "minimum necessary." "Minimum necessary" means that means when you are requesting or disclosing PII, you should only provide enough information to get the job done. If you observe a behavior that may put privacy at risk, you should discuss the matter with your manager.

12. When and to whom do I report a breach?

All incidents and breaches must be reported within one (1) hour of discovery to your IC Information Systems Security Officer and the NIH IT Service Desk. In addition, you should notify your Supervisor, Administrative Officer, Property Officer, and IC Privacy Coordinators as appropriate.

A breach or incident may include:

- The intentional or unintentional release of PII without appropriate consent of the subject

- The loss or theft of a government issued laptop, desktop, cell phone, smart phone, blackberry, USB drive, or any portable device
- The loss or unauthorized use of PII, PHI, Privacy Act or Sensitive Information

13. How can I protect Information at the Office and Teleworking?

Protecting PII and sensitive data in your office or laboratory is important. However, have you also taken the necessary precautions to minimize the risk of improper handling of records when you work offsite from a remote location?

How can I protect information in the office?

- Use the phone to communicate discreetly
- Only store information necessary to do your job
- Physically secure PII in your work area
- Fax information from a secure fax machine
- Use an NIH approved encryption method to send attachments securely via email
- Encrypt removable media, workstations and laptops
- Do not store PII, PHI or Sensitive information on your Government-issued computing or storage device unless it is encrypted
- Ensure your laptop has updated security software
- Never provide personal information to a non-trusted source and double check before giving it to a trusted source
- Shred PII using a cross-cut shredder
- Prior to disposal, deter identity theft by contacting your Property Custodian and/or ISSO to ensure the hard drives of computing and storage devices, to include fax and photocopying machines, are "wiped" clean

How can I protect information while teleworking?

As more organizations allow employees to work remotely or from home, there are increased privacy and security risks.

Supervisors - Establish clear guidelines that will protect personally identifiable and sensitive information from risk. Ensure telework agreements are in place. Document the temporary removal of Government equipment on property loans and/or passes.

Employees/Contractors - You must follow the same secure practices at home that you follow when you are working in the office. Understand why the requirements were created as well as your responsibility to comply with them.

When approved to work from home, a telework center or remote location, take these steps to protect personal information:

- Access the NIH Network from a government computer and Virtual Private Network (VPN)
- Know what personal information you have in your files and on your computer
- Keep only what you need for your work
- Protect the information in your care
- Properly dispose of what you no longer need
- Report privacy and security incidents

NOTE: Staff should NOT send personally identifiable or sensitive NIH information to their personal email accounts or equipment/portable device.

Training

1. Is it mandatory that I take NIH Privacy Awareness training?

- Yes. As mandated by FISMA and OMB Memorandum 07-19[26], all NIH employees and contractors are required to take privacy awareness training. It is imperative that NIH employees possess a general understanding of the importance of privacy protection. Privacy awareness training will also inform NIH staff of relevant privacy policy, guidelines, and procedures. Training must be completed annually.

2. Where do I go to take the NIH Privacy Awareness Training?

- To begin the training, click on the following link, enter your HHS ID badge number and select the appropriate course at the NIH Information Security and Information Management Training Portal (IRT Portal)[27]
- NIH employees should not select the "Public Access to NIH Courses" option located at the bottom left of the screen. If they select that option, they will not receive full credit for the course.

3. What is our HHS ID number?

- It's the Personal Identifier on the back of your NIH ID Badge – XXX-XXXX-XXX. Or, if the font is too small for you to read, you can look up your number by visiting the NIH Employee Directory[28].

4. I can't print a certificate of completion. How do I know if I completed the training?

Follow these steps:

- Visit the NIH Information Security and Information Management Training Portal **If you're an NIH employee**, log on with your NIH badge number (the one associated with both your NED record and AD account) and verify your identity

    - Click "View My Student Record" to confirm you completed the course
    - Scroll down to select 'Privacy Awareness Course' or 'FY Refresher'
    - Click 'View Course Information'
    - Red check marks indicate the modules you have completed
    - Hit Go!

[26] Office of Management and Budget; OMB07-19, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

[27] NIH Information Security and Information Management Training Portal

[28] NIH Employee Directory (NED)

- **If you're a member of the public***, log onto the left side of the screen as a public user, scroll down to select the course and hit Go!

    - You will need to complete the course in one uninterrupted sitting with 30 min or less
    - You will need to complete ALL modules of the course

- From the left column, scroll down and click the button that says Print Certificate
- On the right side, click the Print Certificate icon (it will present you with a window of your certificate)
- Hit the Print button on your computer (the certificate will print with today's date and not the date you took the course)
- Click 'Close'
- Click 'Log Out'
- Close your browser

NOTE: NIH does not maintain a student record of completion on members of the public.

5. Can members of the public take privacy awareness training?

- Yes, the security and privacy awareness courses on the NIH Information Security and Information Management Training Portal are available to the public. NIH does not maintain a student record of completion or track training progress for members of the public. However, if a Public User completes the course in one uninterrupted session (within 30 minutes or less), they can print a certificate of completion. If the session time elapses, they will have to start over upon re-entry. In order for a Public User to be marked as complete, he/she must print off a completion certificate as confirmation and present it to the IC Privacy Coordinator (or other person designated to track training such as the IC Training Coordinator or ISSO).

NIH Third-Party Websites and Applications (TPWAs)

1. When can I use a Third-Party Website and Application?

Although the HHS Center for New Media[29] lists Terms of Service (TOS) agreements that permit use of Third-Party Websites and Applications (TPWA), you must:

- Have a valid, business reason for using social and new media;
- Obtain approval from your Communications Office prior to creating an account;
- Check HHS' Terms of Service (ToS) Agreements page for a Department approved ToS; and
- Complete a TPWA PIA to assess privacy and security risks!

Please refer to NIH Policy on OMA's Manual Chapter webpage[30]:

- MC 2804, NIH Public Facing Web Management
- MC 2805, NIH Web Privacy
- NIH Social Media Guidelines

Social Networking

Web sites (e.g., Facebook, Twitter, YouTube, LinkedIn, Instagram), web tools (e.g., Google Analytics, Project Implicit, Concurrence) and web-based surveys (e.g., SurveyMonkey, SurveyGizmo) are easy to use and available at little or no cost. However, they continue to raise privacy, security and legal concerns.

Federal agencies have no control over the information third-party providers collect. Before the products can be purchased or used, they must be configured to meet government standards.

Check with your IC Communications Director before using any social media tool to communicate a message to the public on behalf of your IC. Check with your ISSO if you need, as part of your job, to access a blocked social media website. Work with OGC to determine if your IC can agree to the legal provisions of the respective "federally friendly" Terms of Service (TOS) agreement negotiated by GSA for use by agencies. Coordinate with other key stakeholders within your IC (e.g., OMA, OCPL, OER, OIR, OHSR) as necessary to determine how your IC can participate in the use of social media. For more information on the policy and guidance of proper usages and approvals for social media and TPWA, please see Manual Chapter 2809.

[29] HHS Center for Media

[30] NIH Office of Management and Assessment Manual Chapters

Cloud Computing

Cloud computing involves the sharing or storage of user information on remote servers owned or operated by others and accessed through internet browsers or other connections. Examples include data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, etc.

NIH staff must weigh the risks, benefits and legal liabilities for exposure of agency data and analyze both the provider being used and the information being put in the cloud.

- Warning: Gmail, Yahoo! and other free email services use cloud services!
- Do the data protections meet the requirements of FISMA?
- Could information in the owner's cloud fall into the hands of a third party? If so, could the information be released without the owner's knowledge?
- Is the cloud provider located in another state or the European Union? If so, the date could be permanently subject to state or EU privacy laws.
- What are the cloud service provider's Terms of Service?
- What sort of security, privacy, and data protection assurances can they provide?
- IMPORTANT: Do NOT forward PII/SI to Gmail and Yahoo! email accounts stored in the cloud.

Healthcare Information Exchanges (HIEs)

HIE is the mobilization of healthcare information electronically across organizations within a region, community or hospital system.

HIE provides the capability to electronically move clinical information among disparate health care information systems while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer and more timely, efficient, effective, and equitable patient-centered care. HIE is also useful to public health authorities to assist in analyses of the health of the population.

HIE systems facilitate the efforts of physicians and clinicals to meet high standards of patient care through electronic participation in a patient's continuity of care with multiple providers.

2. How do I identify a Third-Party Website/Application

To first determine if a Website or web application is a Third Party Website/Application (TPWA), you may access the Health and Human Services (HHS) Center for New Media.
If the Website or application appears on the "Tools with Signed TOS Agreement" list it is a TPWA. The list provides the TPWAs for which HHS has signed a federal-compatible terms of service "TOS" agreement, or for which the standard TOS has been cleared for use. This list is a living document that is regularly updated to reflect the use of new TPWA tools. If a tool is not listed on this list, you should review the TPWA checklist in Manual Chapter 1745-1, *NIH Privacy Impact Assessments*. As well as the NIH Social Media Checklist. As a general rule, if you are considering using a Web-based technology that is not exclusively operated or controlled by NIH or hosted on a .gov domain, it is a TPWA and will require a PIA.

The NIH Office of Communications and Public Liaison lists a number of TPWAs identified by Institute/Center (IC) at the NIH News and Events webpage [31].

Note: The list maintained by the NIH Office of Communications and Public Liaison (link provided above) is only as current as the information provided to them by IC TPWA System Owners/Managers (e.g., staff responsible for opening an account or who handle responses, moderate comments or otherwise have knowledge of the design, development, operation or maintenance of a third-party Website or application).

To further determine if a Website/Application qualifies as a TPWA, apply this six-question litmus test:

1) Is the Website or application part of an authorized law enforcement, national security, or intelligence activity? **Yes** - Other privacy laws will apply to the information collection. Therefore, you do not need to complete a TPWA PIA. **No** - Continue to Question 2.

2) Is the Website or application intended to be used for internal HHS/OPDIV activities only? **Yes** - You do not need to complete a TPWA PIA. However, you are required to complete a PTA. **No** - Continue to Question 3.

3) Does HHS/OPDIV own or have contractual control of the operation or maintenance of the Website or application? **Yes** - You do not need to complete a TPWA PIA. However, you must ensure an IT System PIA was conducted previously on the Website or application (e.g., network, server, or database). **No** - Continue to Question 4.

4) Does another Federal department or agency own or have contractual control of the operation or maintenance of the Website or application? **Yes** - You do not need to complete a TPWA PIA. **No** - Continue to Question 5.

5) Is the Website or application intended to involve members of the public? **Yes** - You need to complete a TPWA PIA. Please collaborate with key stakeholders within your OPDIV, as needed. **No** - Continue to Question 6.

6) Was the Website or application designed for the purpose of implementing the Open Government Directive principles of transparency, participation, and/or collaboration?

Transparency

Providing the public with information about what HHS/OPDIV is doing by making it available online in an open medium or format that can be retrieved, downloaded, indexed, and searched by commonly used web search applications. An open format is one that is platform independent, machine readable, and made available to the public without restrictions that would impede the re-use of that information (e.g., OPDIV Internet Website, Open Government Webpage, Blogs and Social Media Websites that request feedback on and assessment of the quality of published information).

[31] NIH News and Events webpage

Participation

Contribution by the public of ideas and expertise so HHS/OPDIV can make policies with the benefit of information that is widely dispersed in society (e.g., links to Websites where the public can engage in existing participatory processes, mechanisms, innovative tools and practices that create new and easier methods for public engagement in and feedback on the Agency, Department or OPDIV's core mission activities).

Collaboration

The encouragement of partnerships and cooperation with other Federal and non-Federal governmental agencies, the public, and non-profit and private entities in fulfilling the Agency, Department or OPDIV's core mission activities, to include proposed changes to internal management and administrative policies (e.g., technology platforms that improve collaboration among people within and outside HHS/OPDIV, descriptions of and links to appropriate Websites where the public can learn about existing HHS/NIH collaboration efforts, prizes and competitions to obtain ideas from and increase collaboration with those in the private sector, non-profit, and academic communities).

Yes - You need to complete a TPWA PIA. Please collaborate with key stakeholders within your OPDIV, as needed. **No** - It is not a TPWA. **Stop here**.

3. Can NIH prepare one "umbrella" PIA to cover multiple websites or applications that are functionally comparable?

Yes. The OSOP has developed "umbrella" TPWA PIAs to cover multiple third-party websites or applications that are used at NIH for a similar use cases, are functionally comparable and do not raise any distinct privacy risks exclusive to the use of the TPWA. This means that if an ICO or OD office is proposing to use one of the social media tools in the NIH Umbrella TPWAlist, no further action is needed. If, however, the ICO or OD office plans to use a *new* tool for which a PIA has not been completed, please review NIH Manual Chapter 1745-1, Appendix A Checklist.

4. Does HHS maintain a list of websites and applications defined as TPWAs?

No. Due to the fact that the area of Web 2.0 technology is changing rapidly and new technologies are appearing almost daily, the HHS Center for New Media and the HHS Cybersecurity Program do not maintain a comprehensive list of TPWAs. However, the HHS Center for New Media is the best source for technologies that are being used widely since they are often consulted prior to use, and have a list of TPWAs for which HHS has signed a federal TOS agreement.

5. Is there a library of TPWA PIA templates?

HHS does not have a library of templates at this time. However, NIH has posted templates for Facebook, Twitter, Flickr, SurveyMonkey, GovDelivery, and YouTube on the OMA Privacy SharePoint Website. Additional templates will be added in the future.

6. Why are we required to assess TPWAs when we have no contractual control over the operation of the Website or application, nor do we have control over how the third-party uses the information it stores?

Websites under HHS and federal contractual control have contracts between the Federal Government and the contractors (i.e., Challenge.gov) that stipulate certain required information security and privacy activities be conducted. The Federal Government has control over the content on the site and the management of the information collected through the Website. However, the data is not managed by the government once the contract is executed. In general, each government contract includes stipulations for the privacy and security of data utilized and/or collected for a government purpose. Therefore, the privacy policy of the relevant federal agency is posted on these sites.

The government does not control the operations of a third-party Website or application and how that third-party uses information. For example, by virtue of having an account, the government is not in the position to manage how Facebook discloses user data or shares metrics of followers of NIH accounts on Facebook. Therefore, OMB determined federal agencies are responsible for considering the privacy implications of engaging with the public on TPWAs.

7. Do I Need To Conduct A TPWA PIA for the following?

Blogs?

If you create a blog (e.g., Feedback at NIH) through a third-party blogging platform such as Blogger, WordPress, Tumblr etc., you must complete a TPWA PIA. However, be cognizant of the fact that, by using a blogging platform administered by a third-party (even if the blog is embedded on a NIH.gov Website), any information provided by a member of the public on the blog can cause the information—which may contain PII—to be accessible to NIH. However, if the blog is hosted on a NIH.gov Website and does not utilize a third-party blogging platform, a TPWA PIA is not required.

E-mail Subscription Management Services?

If you created a means (e.g., GovDelivery) to allow visitors to provide a personal e-mail address and indicate their subscription preference in order to receive e-newsletters, alerts and other messages, including the items they want to receive, you must complete a TPWA PIA.

Internal Agency Activities *(i.e., SharePoint and Intranet Websites used by employees only)?*

No. Interactions that do not involve the public, or any activity that is part of authorized law enforcement, national security, or intelligence activities, do not need to be assessed with a PIA.

Micro blogs?

If you are using Twitter, Yammer, Posterous, etc. to engage the public, individuals can make personally identifiable information (PII) available or cause it to be accessible to NIH. Therefore, you must complete a TPWA PIA.

HHS Mobile Applications?

Mobile applications installed on a user's device (e.g., iPhone, iPad, iPod) and used to enhance services to employees and the public, through an NIH-owned or operated portable, handheld device are not TPWAs. However, you will need to assess the application and follow the HHS Mobile Applications

Privacy Policy. Including, but not limited to, creating an App-specific Privacy Policy, a Privacy Notification, Privacy Compliance Documentation, and doing a Privacy Risk Assessment.

Online Survey Tools *(i.e., SurveyMonkey, SurveyGizmo, Project Implicit, etc.)?*

Yes. If they engage the public, they are third-party Websites/applications. If they are used to survey NIH employees, you would not conduct a TPWA PIA, only a TPWA PTA is needed. The frequency or lifespan of TPWA use is not a factor. Therefore, a PIA would need to be conducted for each use of the survey tool that makes PII available or could potentially make PII available to NIH.

Podcasts?

If the Podcast is hosted on an intranet site owned by NIH, it does not require the completion of a TPWA PIA. However, if the Podcast is hosted on a third-party Website, or if another music/sound sharing tool owned by a third-party is used to play the podcast, then a TPWA PIA will need to be completed.

RSS Feeds?

If the RSS feed (e.g., Feedburner) is produced by NIH or is hosted on or "lives on" a NIH.gov Website, then a TPWA PIA does not need to be completed. The key is to determine whether the RSS feed uses NIH technology or NIH has contractual control over it. If the RSS feed takes a user to a third-party web feed management provider that provides media distribution and audience engagement services, a TPWA PIA must be completed.

Systems developed by GSA for use by Federal agencies to advertise contests *(i.e., Challenge.gov which goes through Challengepost.com)?*

If the Web address and language indicate the Website is an official U.S. Government Website and NIH does not have control over how information is managed (i.e., no contractual control), you do not need to conduct a TPWA PIA.

Systems developed for use by Federal agencies*?*

If the Web address and language indicate the Website is not an official U.S. Government Website and NIH has control over how information is managed (i.e., contractual control), you must conduct a TPWA PIA.

Vodcasts?

If the vodcast is hosted on an intranet site owned by NIH, it does not require the completion of a TPWA PIA. However, if the vodcast is hosted on a third-party Website such as YouTube, or if another video sharing tool owned by a third-party is used to play the vodcast, then a TPWA PIA is required.

Widgets?

It depends. The functionality of the widget is to allow users to share .gov content on their Facebook, iGoogle or Windows and OS X desktops. If the widget (e.g., AddThis) is used to engage with the public for the purposes of implementing the principles of the Open Government Directive you will need to complete a TPWA PIA.

Wikis?

Wikis are not used by the government to engage with the public for the purpose of implementing the Open Government principles of transparency, participation, or collaboration. In some cases, the government may make contributions to the content, but since the messaging is not controlled by the government, it is not used by the Department to implement the principles of the Open Government Directive. Therefore, Wikis (e.g., Mixed Ink) do not qualify as a TPWA.

8. Are personal e-mail addresses considered to be personally identifiable?

If you create a means for an individual to provide a personal e-mail address (i.e., GovDelivery e-mail subscription service) you should consider that to be personally identifiable (e.g., firstnamelastname@verizon.net). Therefore, Websites and applications that cause an individual to provide an e-mail address, in order to subscribe to a service, should be assessed with a TPWA PIA.

9. Is a personal e-mail address by itself (without a name) considered to be PII?

OMB (M) 07-16 states that PII refers to "**information which can be used to distinguish or trace an individual's identity**, such as their name, social security number, biometric records, etc. **alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual**, such as date and place of birth, mother's maiden name, etc." Therefore, if you can use the information to contact someone, you must consider it to be PII.

10. If we assessed our internet website previously with the IT System PIA and have now modified the system to provide a link to enable the public to download a mobile application from the Apple store, must we now prepare a TPWA PIA on the use of iTunes?

If the public can access the mobile application directly from the iTunes Apps Store (Android Market or other) channel without having to visit the NIH or IC Website, a TPWA PIA must be completed.

11. If we partner with institutions to stand up websites on our behalf for the purpose of registering the public to attend training courses, is the use of the institution website considered to be a third-party?

Yes. If the institution uses a registration service owned by a third-party, or if the Website is not owned or controlled by NIH, it is a third-party Website or application. Please consult your IC Privacy Coordinator and the OSOP to see if a TPWA PIA or an Electronic Information Collection PIA should be completed.

12. If our IC or office has multiple Twitter accounts, do we need to report each use?

Yes. If a NIH office/IC has 12 different *Twitter* (*Facebook*, etc.) accounts, a TPWA PIA must be completed for each account because each represents a unique use of the third-party Website.

NIH Web Measurement and Customization Technologies

1. What is a web measurement and customization technology?

Technologies used to remember a user's online interaction with a Website or online application in order to conduct measurement and analysis of usage or to customize the user's experience

2. What are some examples?

Web bugs, web beacons, and the most common mechanism to track use behavior or customize a Website, session, and persistent cookies.

3. What is the difference between Tier 1, 2, and 3 technologies?

TIER 1

Any use of a ***single-session*** Web measurement and customization technology.

TIER 2

Any use of ***multi-session*** Web measurement and customization technology **w*hen no PII is collected*** (including when the agency is unable to identify an individual as a result of its use of such technologies).

TIER 3

Any use of a ***multi-session*** Web measurement and customization technology ***when PII is collected*** (including when an agency is able to identify an individual as a result of its use).

4. What is meant by a single session technology?

They are technologies that remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not reused, and is deleted immediately after the session ends. An example is a normal web server log that maintains session-only information (whether personally identifiable or not). This includes the collection of an IP address, which the Department views as PII.

5. What is meant by a multi-session technology?

They are technologies that remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.

6. Do I have to conduct a TPWA PIA on Tier 1 usage technologies?

No TPWA PIA is required.

7. Do I have to conduct a TPWA PIA on Tier 2 usage technologies?

No TPWA PIA is required.

8. Do I have to conduct a TPWA PIA on Tier 3 usage technologies?

Yes, you must complete a TPWA PIA on the use of Tier 3 technologies.

9. Do I need to complete a TPWA PIA on all websites?

No. First, consider whether the Website is public-facing. OMB M-10-22[32] applies to web technologies that are used on government-owned or operated Websites, which face the public and collect information from the public. If the web measurement and customization technologies are on a public government Website and collecting information from the public, then M-10-22will apply. If the uses are not on government-owned or operated Websites that face the public, M-10-22 does not apply.

10. Do I have to conduct a TPWA PIA on persistent cookies used to block repeated delivery of surveys (e.g., ACSI customer satisfaction surveys)?

No, not unless they are used on a government-owned or operated Website that faces the public and are used to collect PII.

11. Do I have to conduct a TPWA PIA on persistent cookies used to measure repeat visitors (e.g., WebTrends, Omniture, SiteCatalyst, CrazyEgg, etc.)?

No, not unless they are used on a government-owned or operated Website that faces the public and are used to collect PII.

12. Do I have to conduct a TPWA PIA on tools designed to examine Web traffic and market effectiveness (e.g., Google Analytics, Woopra, etc.)?

These tools are not used to engage the public or convey NIH content to the public. Therefore, you most likely will not have to conduct a PIA. However, depending upon the use of settings, they may qualify as a web measurement or customization technology.

Resources

- Resources can be found at the Federal Privacy Council's website:
  - Law Library
  - Government-wide SORNs
  - OMB Guidance and Memoranda
  - Glossary HHS OCIO Policies
  - NIH OCIO Information Security Policies and Standards

[32] Office of Management and Budget; OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies